pfSense - Bug #6637

pfSense blocks return traffic (mostly TCP) on 2.3.1-RELEASE-p5

07/22/2016 03:19 AM - Remko Lodder

Status:	Resolved	**Start date:**	07/22/2016
Priority:	Normal	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	0%
Category:	Operating System	**Estimated time:**	0.00 hour
Target version:	2.3.2-p1		
Affected Version:	2.2.x	**Affected Architecture:**	

Description

Dear people,

I am setting up a host where I have my AP's connecting to the pfSense box over IPSEC.
I use the "transport" method for that, so that every traffic between the devices is encrypted.

Over that I setup a GIF tunnel (GRE does not seem to work, at this moment), and use OSPF to route the nodes with a default gateway towards the pfSense box.

Now I am hitting an issuse where outgoing TCP traffic over the WAN interface is passing out fine.
The machine also receives the Syn/Ack from the remote host perfectly.
pfSense only immediately sends out a ICMP Host unreachable notice when getting the Syn-Ack back.

I can work around this by disabling the default deny rules:

#---

1. default deny rules
   #---
   block in log inet all tracker 1000000103 label "Default deny rule IPv4"
   block out log inet all tracker 1000000104 label "Default deny rule IPv4"

but then ofcourse the entire firewall is wide open because nothing will be blocked.

This seems like a strange situation, which normally does not occur if you pass traffic (stateful) through a firewall.

Please suggest on what I can do to mitigate this issue.

Thanks
Remko

History

#1 - 07/22/2016 03:25 AM - Remko Lodder

I can narrow this down to the 'block out' rule. (And I believe there is no configurable option, perhaps except on the floating rules, where you can define outgoing rules)

#2 - 07/22/2016 03:20 PM - Chris Buechler

- Category set to Operating System

this seems like it's probably the issue here?
https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=207598

we haven't back-ported that, but it's in FreeBSD 11 so it'll be in 2.4.

#3 - 07/25/2016 01:44 AM - Remko Lodder

Chris Buechler wrote:

> this seems like it's probably the issue here?
> https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=207598
>
> we haven't back-ported that, but it's in FreeBSD 11 so it'll be in 2.4.

hi Chris,

It seems highly relevant indeed. When is 2.4 coming out? Can we update to a snapshot containing this fix already?
It prevents me from using the wireless network in my environment with pfSense (read=showstopper).

#4 - 07/28/2016 01:33 AM - Chris Buechler

- Status changed from New to Confirmed

- Target version set to 2.3.2-p1

- Affected Version set to 2.2.x

There is a known fix for this on PR 207598 that should be easy to import.

all FreeBSD 10.x base versions affected

#5 - 09/26/2016 11:10 AM - Renato Botelho

- Status changed from Confirmed to Feedback

- Assignee set to Renato Botelho

Patch from FreeBSD ticket 207598 was imported to pfSense/FreeBSD-src. Today's 2.3.3-DEVELOPMENT snapshot already has it and can be tested

#6 - 10/06/2016 01:49 PM - Jim Pingle

- Status changed from Feedback to Resolved